Security Enhanced (SE) Android

Stephen Smalley
Trusted Systems Research
National Security Agency

Background / Motivation

- Increasing desire to use mobile devices throughout the US government.
- Increasing interest in Android as an open platform with broad market adoption.
- Need for improved security in mobile operating systems.

What is SE Android?

- A project to identify and address critical gaps in the security of Android.
- A reference implementation produced by the project.
- Initially, enabling and applying SELinux in Android.
- Not limited in scope to SELinux alone.

SE Android is not...

- A government-specific Android.
- A fork of Android.
- A complete solution for all security concerns.
- A product.
- Specially evaluated or approved for use.

SE Android is...

- Security enhancements to Android.
- Addressing platform security.
  - Focused on critical gaps not otherwise being addressed.
- Designed for wide applicability.
- Targeting mainline Android adoption.

SE Android: Use Cases

- Prevent privilege escalation by apps.
- Prevent data leakage by apps.
- Prevent bypass of security features.
- Enforce legal restrictions on data.
- Protect integrity of apps and data.
- Beneficial for consumers, businesses, and government.

How can SELinux help Android?

- Confine privileged daemons.
  - Protect from misuse.
  - Limit the damage that can be done via them.
- Sandbox and isolate apps.
  - Strongly separate apps from one another.
  - Prevent privilege escalation by apps.
- Provide centralized, analyzable policy.


What can't SELinux mitigate?

- Kernel vulnerabilities, in general.
  - Although it may block exploitation of specific vulnerabilities.
- Anything allowed by security policy.
  - Good policy is important.
  - Application architecture matters.
    - Decomposition, least privilege.

Current State

- Working reference implementation
  - originally based on Gingerbread / 2.3.x.
  - now based on Android Open Source Project (AOSP) master branch (4.0.3+)
  - tested on emulator, Nexus S, Motorola Xoom
- Others have tested it on Galaxy Nexus.

Case Studies

- Root exploits
  - Exploid, RageAgainstTheCage, KillingInTheNameOf, GingerBreak, Zimperlich, zergRush, mempodroid
- Flawed apps
  - Skype, Lookout Mobile, Symantec Norton, Wells Fargo, Bank of America, USAA
- Mitigated by SE Android.

Timeline of Events

- First public release Jan 6 2012.
- First submission to AOSP Jan 13.
- bionic patches merged Jan 20.
- libselinux, sepolicy merged Feb 21.
- init/toolbox patches merged Feb 24.
- Remaining patches in progress.

What's Next?

- Finish upstreaming to AOSP.
- MAC for Android permissions.
- Runtime policy management.
- Further integration (kernel and userland).
- Identifying and addressing other security gaps.

Questions?

- http://selinuxproject.org/page/SEAndroid
- SELinux mailing list:
  - selinux@tycho.nsa.gov
- NSA SE Android team:
  - seandroid@tycho.nsa.gov
- My email:
  - sds@tycho.nsa.gov